Subgroups of Groups of Units Modulo n

A THESIS

SUBMITTED TO THE FACULTY OF THE GRADUATE SCHOOL

OF THE UNIVERSITY OF MINNESOTA

BY

Shahriyar Roshan Zamir

IN PARTIAL FULFILLMENT OF THE REQUIREMENTS

FOR THE DEGREE OF

Master of Science

Advisor: Dr. Joeseph Gallian

June, 2019

Acknowledgments

I would like to thank my family for their support and encouragement. A special thanks to UMD's math department; without their support this project would not have been possible. I am grateful for my friends Aaron Victorin-Vangerud and Jiyangyi Qiu; their insightful comments elevated this project. Finally I would like to express my gratitude to my adviser Joe Gallian. This thesis would not have existed without his insight and incredible problem posing ability. Working with him has been, and will always be, one of my greatest mathematical accomplishments. I learned algebra from him but more importantly, he taught me how to be a better human being.

Abstract

The set of all positive integers less than n and relatively prime to n with multiplication mod n is a group denoted $U(n)$. These groups are useful in algebra, number theory and computer science. We are interested in studying the structure of certain subgroups of $U(n)$. As part of their 1980's paper titled *Factoring Groups of Integers Modulo n* Gallian and Rusin determined the structure of $U(n)$ and $U_s(n)$ for $n = st$ where $\gcd(s,t) = 1$ and $U_s(n) = \{x \in U(n) |\ x \pmod{s} = 1\}$. We extend this definition to $U_k(n)$ where k is any positive integer and not necessarily a divisor of n. Moreover for a subgroup H of $U(n)$ and an integer k we define:

$$U_{k,H}(n) = \{x \in U(n) |\ x \pmod{k} \ \in H\}.$$

We find the structure of these subgroups and the factor group $U(n)/U_k(n)$ in terms of an external direct product of cyclic groups. Our methods also determine group elements of $U(n)$ that form a subgroup with a desired structure. We then shift our attention to the class of subgroups defined as:

$$U(n)^{(k)} = \{x^k |\ x \in U(n)\}.$$

We fully classify subgroups of this form and their factor groups. They are useful in finding Sylow p-subgroups of $U(n)$ groups. We also prove some general results about $U(n)$ groups including when the order of $U(n)$ is a power of a prime. Finally we give a simple proof that every finite Abelian group is isomorphic to a subgroup of a U-group.

Contents

1 Group of units of Z_n

1.1 Introduction

For $n \geq 1$, let Z_n denote the cyclic group of order n. The group of units of Z_n ($n > 1$), denoted $U(n)$, is the set of all positive integers less than n and relatively prime to n where the group operation is multiplication mod n. In 1763 Leonhard Euler introduced, for $n > 1$, what is now commonly known as the Euler's phi function $\phi(n)$, also the totient function or phi function, which counts the number of positive integers less than n and relatively prime to n. Hence we will use $|U(n)|$, order of $U(n)$, and $\phi(n)$ interchangeably. In 1801 Gauss gave formulas for calculating $\phi(n)$ in his book "Disquisitiones Arithmeticae." His formulas, although originally expressed in number theory language, help determine the group structure of $U(n)$ in terms of external direct products of cyclic groups when n is a prime power. The groups $U(n)$ have important applications in computer science, data security, cryptography, genetics and electric circuits ([3], 163-167).

In his book "Contemporary Abstract Algebra" [3] Gallian provides in-depth discussions of these groups since they are easy-to-understand examples of groups and a convenient means to demonstrate many concepts. He also introduces and classifies a family of subgroups of $U(n)$; the result of his work with D. Rusin from their 1980 paper titled "Factoring Groups of Integer Modulo n" [4]. For relatively prime positive integers s and t they define $U_s(st) = \{x \in U(st) \mid x \equiv 1(\text{mod } s)\}$. As part of their results, they show that $U(st) \approx U(s) \oplus U(t)$, $U_s(st) \approx U(t)$ and $U_t(st) \approx U(s)$. Their results together with a well-known number theoretic thoerem of Gauss provide an easy way to express any $U(n)$ group as the external direct product of cyclic groups. Their work was explored further in Cheng's 1989 paper titled "Decomposition of U-Groups" [2]. Cheng provides formulas for tracing any element of $U(n)$ in the cyclic group decomposition. The classification of units of the ring Z_n was done by Gauss. In their 2008 paper titled " Classification of Groups of

Units in the Gaussian Integers Modulo n" [1] Allan, Dunne, Jack, Lynd and Ellingsen classify the units of the ring of Gaussian integers mod n. Their paper uses a mixture of group and number theoretic results. In 2019 Gullerud and Mbirika [5] generalized the Euler phi function to Eisenstein integer ring $\mathbb{Z}[\rho]$ where ρ is the primitive third root of unity, $\rho^3 = 1$, by finding the the order of the group of units in the ring $\mathbb{Z}[\rho]/(\theta)$ for any given Eisenstein integer θ. Their paper extends some well-known results in integers and Gaussian integers and shows the Euler-Fermat theorem holds for Eisenstein integers.

Besides the papers listed above, and to the best of author's knowledge, the main approach taken towards studying $U(n)$ groups has been number theoretic. In this paper we use a group theoretic approach to study a certain family of subgroups of $U(n)$. We extend the definition given in [4] and classify the resulting subgroups. We provide a convenient way to give a description of elements of $U(n)$ that form a subgroup with a desired cyclic group structure such as $Z_2 \oplus Z_3$ and Sylow p-subgroups.

1.2 Background Information

In ([3], p.70) Gallian defines, for $n > 1$ and k a positive divisor of n, the subgroup

$$U_k(n) = \{x \in U(n) |\ x \bmod k = 1\}.$$

He gives the example $U_3(21) = \{1, 4, 10, 13, 16, 19\}$. This raises the question "what if the subscript k is not necessarily a divisor of n"? Gallian notes that $U_3(10) = \{x \in U(10) |\ x \bmod 3 = 1\} = \{1, 7\}$ is not a subgroup of $U(10)$. Definition 1.5 provides an alternate way to define $U_k(n)$ so that it is a subgroup of $U(n)$ for all k.

Definition 1.1. [3] *An isomorphism ϕ from a group G to a group $\bar{G}$ is a one-to-one mapping (or function) from G onto $\bar{G}$ that preserves the group operation. That is,*

$$\phi(ab) = \phi(a)\phi(b) \text{ for all } a, b \in G.$$

If there is an isomorphism from G onto $\bar{G}$, we say that G and $\bar{G}$ are isomorphic and write $G \approx \bar{G}$.

Definition 1.2. [3] *Let $G_1, G_2, \ldots, G_n$ be a finite collection of groups. The external direct product of $G_1, G_2, \ldots, G_n$, written as $G_1 \oplus G_2 \oplus \cdots \oplus G_n$, is the set of all n-tuples for which the ith component is an element of G_i and the operation is componentwise.*

In Chapter 8 of [3] Gallian proves that if $gcd(s,t) = 1$ then $U(st) \approx U(s) \oplus U(t)$ under the mapping $\phi(x) \to (x \bmod s,\ x \bmod t)$ and $U_s(st) \approx U(t)$ under the mapping $x \to x \bmod t$. As a corollary to this result we have: if $n = n_1 n_2 \cdots n_r$, where $gcd(n_i, n_j) = 1$ for $i \neq j$, then

$$U(n) \approx U(n_1) \oplus U(n_2) \oplus \cdots \oplus U(n_r).$$

For example $U(105) \approx U(3) \oplus U(5) \oplus U(7)$ under the mapping $x \to (x \bmod 3,\ x \bmod 5,\ x \bmod 7)$. He also notes in the same chapter that $U(p^m) \approx Z_{p^{m-1}(p-1)}$ for an odd prime p. It is important to note the previous result shows $U(p^m)$ is cyclic and has even order for all odd primes p. As an example observe that $U(25) \approx Z_{20}$. Moreover $U(2) \approx \{0\}$, $U(4) \approx Z_2$ and $U(2^n) \approx Z_{2^{n-2}} \oplus Z_2$ for $n \geq 3$. An important observation, which is referred to in Section 1.7, is for that any $n > 2$, the order of $U(n)$ is even. We will frequently refer to the aforementioned results, which are also well known number theory ideas, through out the rest of this paper. We denote $\{1\} \approx Z_1 = \{0\}$; which is why $U(2) \approx \{0\}$. We would like to point out the significant advantage of representing U-groups in terms of external direct product of cyclic groups is that cyclic groups are completely understood and convenient to work with. Even finding the elements of $U(n)$, let alone its structure for large n is tedious by hand.

To show a finite subset of a group is a subgroup, we use the finite subgroups test from

Chapter 3 of Gallian's book [3]. It states that a nonempty finite subset H of a group G that is closed under the operation of G is a subgroup of G. Let us use this test to show $U_k(n) = \{x \in U(n) |\ x = kt + 1 \pmod{n} \text{ for } t \in \mathbb{Z}\}$ is indeed a subgroup of $U(n)$. The nonempty condition follows since $1 \in U_k(n)$. Let $x, y \in U_k(n)$. Then $x = kt_1 + 1 \pmod{n}$, $y = kt_2 + 1 \pmod{n}$ and $xy = k(kt_1t_2 + t_1 + t_2) + 1 \pmod{n}$, so $U_k(n)$ is a subgroup of $U(n)$.

Definition 1.3. [3] *A group G is the internal direct product of H and K, denoted $G = H \times K$, if H and K are normal subgroups of G, $G = HK$ and $H \cap K = \{e\}$. Moreover $G = H \times K$ implies $G = H \oplus K$.*

Proposition 1.4. *Let $G \approx Z_{p_1^{n_1}} \oplus \cdots \oplus Z_{p_k^{n_k}}$ and H be a subgroup of G such that $|H| = p_1^{n_1 - m_1} \cdots p_k^{n_k - m_k}$ where p_i is prime and $0 \leq m_i \leq n_i$ for all i. Then $G/H \approx Z_{p_1^{m_1}} \oplus \cdots \oplus Z_{p_k^{m_k}}$.*

Proof. Note G is k-generated therefore $G =< g_1, \ldots, g_k >$ where $|g_i| = p_i^{n_i}$. Let H be a subgroup of G and consider the natural homomorphism $\phi : G \to G/H$ given by $\phi(g) = gH$. We want to show $G/H =< g_1H, \ldots, g_kH >$. Let $gH \in G/H$. Observe that $g = g_1^{a_1} \cdots g_k^{a_k}$ implies $\phi(g) = gH = \phi(g_1^{a_1}) \cdots \phi(g_k^{a_k}) = (g_1H)^{a_1} \cdots (g_kH)^{a_k}$.
Therefore $G/H =< g_1H, \ldots, g_kH >$. Given the order of g_iH divides the order of g_i for all i, let $|g_iH| = p_i^{m_i}$. This implies $G/H \approx Z_{p_1^{m_1}} \oplus \cdots \oplus Z_{p_k^{m_k}}$ where $p_i^{m_i}$ divides $p_i^{n_i}$ for all i. □

1.3 Results related to $U_k(n)$

Definition 1.5. *Let $n > 1$ and k be any integer.*
Then $U_k(n) = \{x \in U(n) |\ x = kt + 1$ (mod n) for $t \in \mathbb{Z}\}$ is a subgroup of $U(n)$.

When k divides n this definition agrees with the one in [3], provided at the beginning of Section 1.2, but it defines a subgroup for all k. Henceforth Definition 1.5 will be our

definition for $U_k(n)$ because it leads to a natural generalization in Section 1.5. Using this new definition we get:

$$U_3(10) = \{1, 7, 3, 9\}$$

$$U_6(15) = \{1, 7, 13, 4\}$$

$$U_{24}(60) = \{1, 49, 13, 37\}$$

$$U_{15}(70) = \{1, 31, 61, 51, 11, 41\}$$

$$U_{15}(9) = \{1, 4, 7\}$$

$$U_{20}(15) = \{1, 11\}.$$

The subgroup $U_k(n)$ is every element of $U(n)$ that is $1 \pmod k$. To find its elements, add 1 to integer multiples of k, mod by n, and check if the result is relatively prime to n. If so, keep that integer, if not, move to the next multiple. Continue this process until you get back to 1. Using modular arithmetic allows us to assume t is non-negative. For example in $U_{24}(60)$, $0 \cdot 24 + 1$ is relatively prime to 60 but $1 \cdot 24 + 1$ is not. The point is we do not need to know all the elements of $U(n)$ to find the subgroup $U_k(n)$. Although this definition appears to be more general, Theorem 1.6 shows that compared to taking a divisor k, it does not introduce a new subgroup of a U-group.

Our first example, $U_3(10)$, is the whole group $U(10)$ and $\gcd(10, 3) = 1$. Observe in the second example that $U_6(15) = U_3(15) \cap U_2(15) = U_3(15) = \{1, 4, 7, 13\}$ since $U_2(15) = U(15)$ (by checking the elements). It is no coincidence that $\gcd(15, 6) = 3$.

Theorem 1.6. *Let n and k be positive integers with $n > 1$. If $gcd(k, n) = 1$ then $U_k(n) = U(n)$. Moreover, $U_k(n) = U_{gcd(n,k)}(n)$.*

Proof. First we show that if $gcd(k, n) = 1$ then $U_k(n) = U(n)$. By definition, $U_k(n) \subseteq U(n)$. Suppose $x \in U(n)$. If $x = 1$, then $x \in U_k(n)$. Assume $1 < x < n$. For some

integers a, b we have $ak + bn = 1$. Multiplying both sides by $x - 1$ and solving for x we get $a'k + b'n + 1 = x$ where $a' = (x - 1)a$ and $b' = (x - 1)b$. Taking mod n on both sides, we see that x has the desired form, therefore $U(n) \subseteq U_k(n)$. For the second part, if k is a divisor of n, the result is trivial. Suppose k is not a divisor of n. Let $\gcd(k, n) = d$ where $k = dh$ and $\gcd(h, n) = 1$. By definition $U_k(n) = U_d(n) \cap U_h(n) = U_d(n)$ since $U_h(n) = U(n)$. □

We provide a second proof that directly shows $U_k(n) = U_{gcd(n,k)}(n)$. Let $gcd(k, n) = d$, $k = dh$, and $x \in U_k(n)$. Then $x = kt + 1$ (mod n) implies $x = d(ht) + 1$ (mod n) which is in $U_d(n)$. For $x \in U_d(n)$ we have $x = dt' + 1$ (mod n). We know there exists integers s and t such that $sk + tn = d$. Therefore $x = (sk + tn)t' + 1 \equiv k(st') + 1$ (mod n). This completes the proof.

Because of Theorem 1.6 we may now assume, without loss of generality, that for all subgroups of the form $U_k(n)$, k is a positive divisor of n. This result shows any factor of k in $U_k(n)$ that is relatively prime to n can be "canceled."

Theorem 1.13 classifies all subgroups of the form $U_k(n)$ where $n > 1$. Although Lemma 1.7 and Lemma 1.10 are not directly used in the proof of Theorem 1.13, they help this classification. For the proof of Lemma 1.7 and Proposition 1.9, recall that every subgroup and every factor group of a cyclic group is cyclic.

Lemma 1.7. *For an odd prime p and $1 \leq k \leq m$ we have $U_{p^k}(p^m) \approx Z_{p^{m-k}}$.*

Proof. Note $|U_{p^k}(p^m)| = p^{m-k}$ from the observation that $U_{p^k}(p^m) = \{1, p^k + 1, \ldots, (p^{m-k} - 1)p^k + 1\}$ and since $U(p^m)$ is cyclic, the result follows. □

Example 1.8. Let $n = 11^5$ and $k = 11^3$. Then $U_{11^3}(11^5) \approx Z_{121}$ and $U_{11^5}(11^5) \approx Z_1$. This is significant since it allows us to get the structure of $U_{p^k}(p^m)$ in terms of a cyclic group.

Proposition 1.9. *For an odd prime p and $1 \leq k \leq m$, we have $U(p^m)/U_{p^k}(p^m) \approx Z_{p^{k-1}(p-1)}$.*

Proof. We only need to find the order of $U(p^m)/U_{p^k}(p^m)$, which is

$$|U(p^m)/U_{p^k}(p^m)| = \frac{p^{m-1}(p-1)}{p^{m-k}} = p^{k-1}(p-1).$$

□

Lemma 1.10. *Let $n \geq 1$ and $2 \leq i \leq n$. Then $U_2(2^n) = U(2^n)$, $U_{2^n}(2^n) = \{1\}$ and $U_{2^i}(2^n) \approx Z_{2^{n-i}}$.*

Proof. Clearly $U_2(2^n) \subseteq U(2^n)$. For any $x \in U(2^n)$, x is odd which implies $x \equiv 1 \pmod 2$ therefore $x \in U_2(2^n)$.

Observe that $|U_{2^i}(2^n)| = 2^{n-i}$ because $U_{2^i}(2^n) = \{1, 2^i + 1, \ldots, (2^{n-i} - 1)2^i + 1\}$. Since $U_{2^i}(2^n)$ is a subgroup of $U(2^n) \approx Z_2 \oplus Z_{2^{n-2}}$, then $U_{2^i}(2^n)$ is isomorphic to either $Z_{2^{n-i}}$ or $Z_2 \oplus Z_{2^{n-i-1}}$. This implies the subgroup $U_{2^i}(2^n)$ has either one or three elements of order 2. We will show it has one. Note the group $U(2^n)$ has exactly three elements of order 2, namely $2^n - 1$ and $2^{n-1} \pm 1$. If $2^n - 1 \in U_{2^i}(2^n)$ then $2^n - 1 = k \cdot 2^i + 1$ for some integer k. This is a contradiction since the left hand side is -1 mod (2^i) and right hand side is 1 mod (2^i). So $U_{2^i}(2^n)$ has only one element of order 2, and therefore is isomorphic to $Z_{2^{n-i}}$. □

Proposition 1.11 gives the structure of $U(2^n)/U_{2^i}(2^n)$. The proof uses Proposition 1.4 which states that if $G \approx Z_{p_1^{n_1}} \oplus \cdots \oplus Z_{p_k^{n_k}}$ then $G/H \approx Z_{p_1^{m_1}} \oplus \cdots \oplus Z_{p_k^{m_k}}$ where H is a subgroup of G, p_i is a prime and $0 \leq m_i \leq n_i$ for all i.

Proposition 1.11. *If $n = i$ then $U(2^n)/U_{2^i}(2^n) \approx Z_1$. For $n = 2$ and $i = 1$ we have $U(4)/U_2(4) \approx Z_1$. For $2 \leq i < n$ we have $U(2^n)/U_{2^i}(2^n) \approx Z_2 \oplus Z_{2^{i-2}}$.*

Proof. The first two assertions are obvious. So we assume that $2 \leq i \leq n$. Note $|U(2^n)/U_{2^i}(2^n)| = 2^{i-1}$. By Proposition 1.4, $U(2^n)/U_{2^i}(2^n)$ is isomorphic to either $Z_{2^{i-1}}$ or $Z_2 \oplus Z_{2^{i-2}}$ and therefore it has either one or three elements of order 2. We will show the latter is the case by exhibiting two elements of order 2. Let $H = U_{2^i}(2^n)$. Clearly

$|(2^n-1)H| = 1$ or 2. Suppose $2^n - 1 \in H$. Then $2^n - 1 = 2^i \cdot k + 1$ but that's impossible since the left side is $-1 \pmod{2^i}$ and the right side is $1 \pmod{2^i}$. Similarly we can show that $|(2^{n-1}-1)H| = 2$. □

Lemma 1.12. *$U_{2h}(n) = U_h(n)$ where h is odd.*

Proof. By Theorem 1.6 we can assume $2h$ divides n therefore n is even. It follows from the definition that $U_{2h}(n) \subseteq U_h(n)$. Let $x \in U_h(n) = \{hk + 1 (\text{mod } n) \mid k \in \mathbb{Z}\}$. Since h divides n, we don't have to worry about mod-ing by n. Because we will get back to 1 before getting $x = hk' + 1$ where x larger than n. Therefore $x = hk + 1$. If k is odd, then x is even and hence not relatively prime to n therefore k has to be even. Let $k = 2t$. Then $x = 2h(t) + 1$ therefore $x \in U_{2h}(n)$. □

Theorem 1.13. *Let $p_1, \ldots, p_k$ be distinct primes. For $1 \leq m_i$, $0 \leq j_i \leq m_i$, $1 \leq i \leq k$, we have $U_{p_1^{j_1} \cdots p_k^{j_k}}(p_1^{m_1} \cdots p_k^{m_k}) \approx U_{p_1^{j_1}}(p_1^{m_1}) \oplus \cdots \oplus U_{p_k^{j_k}}(p_k^{m_k})$.*

Proof. We know from [3] (p.160) that $U(p_1^{m_1} \cdots p_k^{m_k})$ is isomorphic to $U(p_1^{m_1}) \oplus \cdots \oplus U(p_k^{m_k})$ under the mapping $\phi(x) = (x \pmod{p_1^{m_1}}, \ldots, x \pmod{p_k^{m_k}})$. We will show that the same mapping is the required isomorphism. For convenience, let $a = p_1^{m_1} \cdots p_k^{m_k}$ and $b = p_1^{j_1} \cdots p_k^{j_k}$. If b is divisible by 2 and not 4, then by Lemma 1.12 we can neglect that factor of 2 in b. So, we may assume that if b is even, then b is divisible by at least 4. The restriction of the domain of ϕ from $U(a)$ to $U_b(a)$ is a well-defined, one-to-one and operation preserving mapping from $U_b(a)$ to $U_{p_1^{j_1}}(p_1^{m_1}) \oplus \cdots \oplus U_{p_k^{j_k}}(p_k^{m_k})$ because ϕ is an isomorphism. We only need to show this mapping is onto. Since ϕ is a one-to-one mapping, we only need to show that $\phi(U_b(a))$ is into $U_{p_1^{j_1}}(p_1^{m_1}) \oplus \cdots \oplus U_{p_k^{j_k}}(p_k^{m_k})$ and they have the same order. It follows, from Definition 1.5 and Lemma 1.12, that the order of $U_b(a) = \dfrac{a}{b} = p_1^{m_1 - j_1} \cdots p_k^{m_k - j_k}$. (In the case of b even, the previous assumption of b being divisible by at least 4 was necessary for this and the next claim.)

By Theorem 1.6, we have:

$$|U_{p_1^{j_1}}(p_1^{m_1})| = p_1^{m_1-j_1}$$

$$\vdots$$

$$|U_{p_k^{j_k}}(p_k^{m_k})| = p_k^{m_k-j_k}.$$

Therefore the order of $U_{p_1^{j_1}}(p_1^{m_1}) \oplus \cdots \oplus U_{p_k^{j_k}}(p_k^{m_k}) = p_1^{m_1-j_1} \cdots p_k^{m_k-j_k}$. To show the into part, let $x \in U_b(a)$. Note $\gcd(p_i, x) = 1$ for all i since $\gcd(a, x) = 1$. Moreover $\phi(x) = (x \pmod{p_1^{m_1}}, \cdots, x \pmod{p_k^{m_k}})$. To show $\phi(x)$ is in $U_{p_1^{j_1}}(p_1^{m_1}) \oplus \cdots \oplus U_{p_k^{j_k}}(p_k^{m_k})$, mod the i-th component by $p_i^{j_i}$. This yields

$$(x \pmod{p_1^{m_1}} \pmod{p_1^{j_1}}, \cdots, (x \pmod{p_k^{m_k}} \pmod{p_k^{j_k}}) =$$

$$(x \pmod{p_1^{j_1}}, \cdots, x \pmod{p_k^{j_k}}) = (1, \cdots, 1)$$

since $x \equiv 1 \pmod{b}$. □

The following corollaries are direct consequences of Theorem 1.13, Lemma 1.7, and Lemma 1.10.

Corollary 1.14. *If $|U_k(n)| = p^m$ for an odd prime p and $1 \leq m$ then $U_k(n) \approx Z_{p^m}$.*

Corollary 1.15. *Let $p_1, \ldots, p_k$ be distinct odd primes. For $1 \leq j_i \leq m_i$ and $1 \leq i \leq k$, we have $U_{p_1^{j_1} \cdots p_k^{j_k}}(p_1^{m_1} \cdots p_k^{m_k}) \approx Z_{p_1^{m_1-j_1} \cdots p_k^{m_k-j_k}}$.*

In Theorem 2.7 we give a generator for $U_{p_1^{j_1} \cdots p_k^{j_k}}(p_1^{m_1} \cdots p_k^{m_k})$.

To demonstrate how we can use Theorem 1.13, suppose we want to find the structure of $U_{140}(1800)$. Finding each element and its order would be tedious and not insightful. Instead we have $U_{140}(1800) = U_{20}(1800)$ and by Theorem 1.13 we get $U_{20}(1800) \approx U_4(8) \oplus U_5(25) \oplus U(9) \approx Z_2 \oplus Z_5 \oplus Z_6$.

Example 1.16 demonstrates how we can reverse the process in Theorem 1.13. That is, instead of starting with a subscript k and finding the structure of $U_k(n)$, we look at the structure of $U(n)$ in terms of external direct product of cyclic groups, pick a certain structure in the direct product and find a subscript k such that $U_k(n)$ yields the desired structure. This gives us specific elements in the big group that yield that subgroup structure.

Example 1.16. Let $n = 2^4 \cdot 3^2 \cdot 7^2 = 7056$ and suppose we want to find a cyclic subgroup of order 12 in $U(7056)$. We know $U(7056) \approx U(16) \oplus U(9) \oplus U(49) \approx Z_2 \oplus Z_4 \oplus Z_6 \oplus Z_{42}$ and $Z_{12} \approx Z_4 \oplus Z_3$. We want to pick the subscript to get the $Z_4 \oplus Z_3$ structure in $U(n)$. Consider $U_4(16) \oplus U_3(9) \oplus U_{49}(49)$. The first two components yield four and three elements respectively and the last piece is eliminated. Therefore $U_4(16) \oplus U_3(9) \oplus U_{49}(49) \approx Z_4 \oplus Z_3$ and by Theorem 1.13 we have $U_4(16) \oplus U_3(9) \oplus U_{49}(49) \approx U_{588}(7056)$. This implies $U_{588}(7056) \approx Z_{12}$, which means elements of $U(7056)$ that are $1 \pmod{588}$ make a cyclic subgroup of order 12. In some sense, we have given a description of a cyclic subgroup of order 12 in $U(7056)$. Note this is not possible for every possible subgroup of $U(n)$. We discuss this in detail later on.

In Theorem 1.6 we proved $U_k(n) = U(n)$ if $\gcd(k, n) = 1$. Is this the only case when $U_k(n) = U(n)$? Almost! Theorem 1.18 answers this question. But first we need the following facts.

Lemma 1.17. $|U_{2^i}(2^m)| < |U(2^m)|$ *when* $2 \leq i \leq m$.

Proof. Follows directly from Lemma 1.10. □

Theorem 1.18. *For* $1 \leq k \leq n$ *we have* $U_k(n) = U(n)$ *if and only if* $gcd(n, k) = 1$ *or* 2.

Proof. We've already proved the case where $gcd(k, n) = 1$. Let $gcd(k, n) = 2$. By Theorem 1.6 and Lemma 1.12 we get $U_k(n) = U_2(n) = U(n)$.
Now suppose $U_k(n) = U(n)$ which implies $|U_k(n)| = |U(n)|$. Let $gcd(k, n) = d$. Theorem 1.6 implies $U_k(n) = U_d(n) = U(n)$. Assume for the sake of contradiction, that

$3 \leq d \leq n$. We will draw a contradiction by showing $|U_d(n)| < |U(n)|$. If d is a power of 2 then Lemma 1.17 yields $|U_d(n)| < |U(n)|$, which is a contradiction. If d is not a power of 2 and $3 \leq d$ we use Theorem 1.13 and decompose $U_d(n)$ into its "external direct product pieces" as stated in Theorem 1.13. There will then be *at least* one term of the form $U_p(p^i)$ where p is an odd prime. By Lemma 1.7, we then see that $|U_p(p^i)| < |U(p^i)|$ but $U(p^i)$ will be a term in the decomposition of $U(n)$. This implies $|U_d(n)| < |U(n)|$, which is a contradiction. □

We conclude this section by finding the structure of $U(n)/U_k(n)$ for any k and n.

Theorem 1.19. *Let $n > 1$ be an odd integer and k a divisor of n. Then $U(n)/U_k(n) \approx U(k)$.*

Proof. Let $n = p_1^{n_1} \cdots p_j^{n_j}$ and $k = p_1^{m_1} \cdots p_j^{m_j}$. Consider the homomorphism $\phi : U(n) \to U(k)$ given by $\phi(x) = x \pmod{k}$. We know $\text{Ker}(\phi) = U_k(n)$ since it contains all elements of $U(n)$ that are $1 \pmod{k}$ by Definition 1.5. By the first isomorphism theorem we know $U(n)/U_k(n) \approx \phi(U(n))$. Moreover, $\phi(U(n))$ is a subgroup of $U(k)$. We will show $|\phi(U(n))| = |U(k)|$. Note $|U(k)| = \phi(k) = p_1^{m_1-1}(p_1 - 1) \cdots p_j^{m_j-1}(p_j - 1)$. It follows from Theorem 1.13 and Lemma 1.7 that $|\phi(U(n))| = |U(n)/U_k(n)| = \dfrac{|U(n)|}{|U_k(n)|} = \dfrac{p_1^{n_1-1}(p_1 - 1) \cdots p_j^{n_j-1}(p_j - 1)}{p^{n_1-m_1} \cdots p^{n_j-m_j}} = p_1^{m_1-1}(p_1 - 1) \cdots p_j^{m_j-1}(p_j - 1)$. □

Corollary 1.20. *If n is even and 4 divides k, then $U(n)/U_k(n) \approx U(k)$.*

Proof. The argument is identical to the proof Theorem 1.19. To find the order of $U(n)/U_k(n)$ we use Lemma 1.7 and Lemma 1.10. □

Corollary 1.21. *If n is even and $k = 2h$ where h is odd, then $U(n)/U_k(n) \approx U(h)$.*

Proof. We know from Lemma 1.12 that $U_k(n) = U_h(n)$ and since h is odd, the result follows from Theorem 1.19. □

1.4 Results related to $U_{\pm k}(n)$

Does every subgroup of $U(n)$ have a representation of the form $U_k(n)$ where k is a divisor of n? The answer is no. For example $U(36)$, which is isomorphic to $Z_2 \oplus Z_6$, has a subgroup with $Z_2 \oplus Z_2$ structure. However for no divisor k of 36 do we get $U_k(36) \approx Z_2 \oplus Z_2$. This motivates our next definition, a modification of Definition 1.5. It will help us give a description of the elements of $U(36)$ which form the subgroup $Z_2 \oplus Z_2$.

Definition 1.22. *For $n > 1$ and a positive integer k, we define*

$$U_{\pm k}(n) = \{x \in U(n) |\ x = kt \pm 1 \ (\textit{mod}\ n) \textit{ for } t \in \mathbb{Z}\}\,.$$

This is a subgroup of $U(n)$. Since $1 \in U_{\pm k}(n)$, it is nonempty. Because our set is finite, we only need to check for closure. Let $x, y \in U_{\pm k}(n)$. We have $x = km_1 \pm 1$ and $y = km_2 \pm 1$. Note that $xy \in U(n)$ and $xy = k(km_1m_2 \pm m_1 \pm m_2) \pm 1$. Therefore xy has the desired form. Moreover $U_k(n)$ is always a subgroup of $U_{\pm k}(n)$. An equivalent definition of this subgroup is:

$$U_{\pm k}(n) = \{x \in U(n) |\ x \bmod k \in \{1, -1\}\}\,.$$

The first definition is used to generate subgroups of the form $U_{\pm k}(n)$. The advantage of the second definition is it suggests a natural generalization that we will introduce in Section 1.5. We hope to provide a deeper understanding of these subgroups by first focusing on the special case of $U_{\pm k}(n)$ and its related results. A few examples of $U_{\pm k}(n)$ are:

$$U_{\pm 9}(36) = \{1, 17, 19, 35\}$$

$$U_{\pm 11}(33) = \{1, 10, 23, 32\}$$

$$U_{\pm 13}(52) = \{1, 25, 27, 51\}$$

$$U_{\pm 3}(36) = \{1, 5, 7, 11, 13, 17, 19, 23, 25, 29, 31, 35\}$$

$$U_{\pm 5}(45) = \{1, 4, 11, 14, 16, 19, 26, 29, 31, 34, 41, 44\}.$$

The first example answers our question about a subgroup of order four in $U(36)$, that is $U_{\pm 9}(36) \approx Z_2 \oplus Z_2$. As was the case with $U_k(n)$, we don't need to know all of the elements of $U(n)$ to find the elements of $U_{\pm k}(n)$. The algorithm is similar. Add and subtract 1 from all non-negative integer multiples of k and then mod by n. Check to see if the result is relatively prime to n. Continue in this fashion until you're back to 1. For example $1 \cdot 9 + 1 \pmod{36}$ is not relatively prime to 36 so we discard it.

As mentioned previously, Gallian [3] proved $U_s(st) \approx U(t)$. The following proposition extends this idea to the subgroup introduced in this section.

Proposition 1.23. *Let $n = st$ where $gcd(s, t) = 1$. Then $U_{\pm s}(n) \approx U_s(n) \times \{1, n-1\} \approx U(t) \oplus Z_2$.*

Proof. From [3] we know if $G = H \times K$ then $G = H \oplus K$. By observation $U_{\pm s}(n) = U_s(n) \times \{1, -1\}$, where $-1 \equiv n - 1 \pmod{n}$. (A detailed and more general proof of why the two subgroups $U_{\pm s}(n)$ and $U_s(n) \times \{1, -1\}$ are equal is given in Theorem 1.24.) Moreover $U_s(n) = U_s(st) \approx U(t)$ and $\{1, -1\} \approx Z_2$. Therefore $U_{\pm s}(n) \approx U(t) \oplus Z_2$. □

Is $U_{\pm k}(n) = U_k(n) \times \{1, -1\}$ for all $1 \leq k \leq n$? The answer is "almost" again! In Theorem 1.18 we proved that $U_k(n) = U(n)$ if and only if $\gcd(k, n) = 1$ or 2. In the next theorem, we tie this result to subgroups of the form $U_{\pm k}(n)$ to determine their structure. We show that if Theorem 1.18 is not satisfied, then the structure of $U_{\pm k}(n)$ is similar to that of $U_k(n)$ with a Z_2 term.

Theorem 1.24. *For $1 \leq k \leq n$, $U_k(n) = U(n)$ or $U_{\pm k}(n) = U_k(n) \times \{1, -1\} \approx U_{gcd(k,n)}(n) \oplus Z_2$.*

Proof. For $1 \leq k \leq n$, if $U_k(n) = U(n)$ we are done; which by Theorem 1.18 is true if and only if $gcd(k, n) = 1$ or 2. Suppose $U_k(n) \neq U(n)$. It suffices to show $U_{\pm k}(n) = U_k(n) \times \{1, -1\}$. (The rest follows from Theorem 1.6.) Let $A = U_{\pm k}(n)$ and $B = U_k(n) \times \{1, -1\}$. The assumption that $U_k(n) \neq U(n)$ allows for set B to exist. Otherwise the notion of internal direct product would not make sense. Because both A and B are subgroups of $U(n)$, it suffices to show A and B are subsets of each other. For $x \in A$, if $x = kt + 1$ then we are done. If $x = kt - 1$ then $x = -(k(-t) + 1)$, which is an element of B. Now let $x \in B$. If $x = (kt+1)(1)$ then we are done. If $x = (kt+1)(-1)$ then $x = k(-t)-1$ which is an element of A. Finally we get $U_{\pm k}(n) = U_k(n) \times \{1, -1\} \approx U_{gcd(k,n)}(n) \oplus Z_2$. □

The following examples demonstrates how the above results taken together can shorten calculations. As Gallian says in his book "theorems are labor saving devices."

Example 1.25. Consider $n = 3 \cdot 5 \cdot 7^2 = 725$ and $k = 11 \cdot 7 = 77$. Suppose we want to find the structure of $U_{\pm 77}(735)$. It would be cumbersome to find all the elements of $U_{\pm 77}(735)$, let alone it's structure. Instead we note that $\gcd(735, 77) = 7$ which implies $U_{\pm 77}(735) = U_{77}(735) \times \{1, -1\} = U_7(735) \times \{1, -1\} \approx U_7(735) \oplus Z_2 \approx U(4) \oplus U(5) \oplus U_7(49) \oplus Z_2 \approx Z_2 \oplus Z_4 \oplus Z_7 \oplus Z_2 \approx Z_{28} \oplus Z_2 \oplus Z_2$.

Example 1.26. Let's look at the more intimidating case of $n = 2^3 \cdot 3^3 \cdot 5^2 \cdot 11 = 569400$ and $k = 2^2 \cdot 3 \cdot 5 \cdot 13 = 780$ and find the structure of $U_{\pm 780}(59400)$. Note that $\gcd(59400, 780) = 60$ which implies $U_{\pm 780}(59400) \approx U_{780}(59400) \oplus Z_2 \approx U_4(8) \oplus U_5(25) \oplus U_3(27) \oplus U(11) \oplus Z_2 \approx Z_2 \oplus Z_5 \oplus Z_9 \oplus Z_{10} \oplus Z_2 \approx Z_{45} \oplus Z_{10} \oplus Z_2 \oplus Z_2$.

We now ask the following question: does every subgroup of a $U(n)$ group has a representation of the form $U_{\pm k}(n)$ or $U_k(n)$? The answer is again no. For example in $U(252) \approx Z_2 \oplus Z_6 \oplus Z_6$ has no divisor k such that $U_k(252)$ or $U_{\pm k}(252)$ yields the subgroup $Z_2 \oplus Z_2 \oplus Z_2$ in the big group $U(252)$. This question motivates a new way producing subgroups in a $U(n)$ group introduced in Section 1.6.

1.5 Results related to $U_{k,H}(n)$

Recall the second definition of $U_{\pm k}(n)$ given at the beginning of Section 1.4:

$$U_{\pm k}(n) = \{x \in U(n) |\ x \bmod k \in \{1, -1\}\}.$$

Note that $\{1, -1\}$ is a subgroup of $U(n)$ for $n > 1$. To generalize this definition we replace $\{1, -1\}$ with any subgroup H of $U(n)$.

Definition 1.27. *For $n > 1$, let k be a positive divisor of n and H be a subgroup of $U(n)$. We define $U_{k,H}(n) = \{x \in U(n) |\ x$ mod $k \in H\}$.*

We next introduce yet another alternative definition for this of type of subgroups because in our experience, the first definition, even though compact and aesthetically pleasing, can be hard to work with. For $n > 1$, k a positive divisor of n and H a subgroup of $U(n)$, we define

$$U_{k,H}(n) = \{x \in U(n) |\ x = kt + h \pmod{n},\ h \in H \text{ and } t \in \mathbb{Z}\}.$$

Our next proposition shows the set defined above is indeed a subgroup of $U(n)$

Proposition 1.28. *The set $U_{k,H}(n)$ is a subgroup of $U(n)$.*

Proof. Since $1 \in U_{k,H}(n)$ we see that it is nonempty. Let $x, y \in U_{k,H}(n)$. Then $x, y \in U(n)$ and $x = kt_1 + h_1 \pmod{n}$ and $y = kt_2 + h_2 \pmod{n}$ for $h_1, h_2 \in H$. Observe that $xy \in U(n)$ and $xy = k(kt_1t_2 + t_1h_2 + t_2h_1) + h_1h_2 \pmod{n}$. Because H is a subgroup of $U(n)$ we have $h_1h_2 \in H$. Therefore xy has the desired form and by the finite subgroup test we are done. □

The advantage of using these subgroups is that by picking a positive divisor k of n and a subgroup H of $U(n)$ we are able to construct a new subgroup of $U(n)$, by changing the divisor k or the subgroup H (or both) we can get more subgroups of $U(n)$. Finally, recall the

definitions $U_k(n) = \{x \in U(n) |\ x = kt + 1,\ t \in \mathbb{Z}\}$ and $U_{\pm k}(n) = \{x \in U(n) |\ x = kt \pm 1 \pmod{n}$ for t
Note if we let $H = \{1\}$ or $H = \{1, -1\}$ the definition of $U_{k,H}(n)$ agrees with the definition of $U_k(n)$ and $U_{\pm k}(n)$ respectively. Here is an example of a subgroup of the form $U_{k,H}(n)$.

Example 1.29. Let $n = 80$, $k = 10$ and $H = \{1, 9\}$. Then we get $U_{10,\{1,9\}}(80) = \{x \in U(80) |\ x = 10t + 1$ or $x = 10t + 9,\ t \in \mathbb{Z}\}$. For $t = 0$, we get H back. For $t = 1$ we get 11 and 19. For $t = 2$ we get 21 and 29 and so on. Note we only need to check up to $t = 8$. Observe $U_{10,\{1,9\}}(80) = \{1, 9, 11, 19, 21, 29, 31, 39, 41, 49, 51, 59, 61, 69, 71, 79\}$, which is indeed a subgroup of $U(80)$.

In view of Theorem 1.24 it is natural to wonder when $U_{k,H}(n) = U_k(n) \times H$. Theorem 1.30 answers this question.

Theorem 1.30. *Let $n > 1$, k a positive divisor of n and H a subgroup of $U(n)$. Then $U_{k,H}(n) = U_k(n) \times H$ if and only if $U_k(n) \cap H = \{1\}$.*

Proof. Suppose $U_k(n) \cap H = \{1\}$. It suffices to show $U_{k,H}(n) = U_k(n)H$ since the rest follows from the definition of internal direct product. For $x \in U_k(n)H$, we have $x = (kt + 1)h \pmod{n} = k(th) + h \pmod{n}$, which is an element of $U_{k,H}(n)$. Let $x \in U_{k,H}(n)$, then $x = kt + h$ for $h \in H$. The following chain of equalities shows $x \in U_k(n)H$;

$$x = (kt + h)1 = (kt + h)h^{-1}h = (k(th^{-1}) + 1)h.$$

Therefore x has the desired form. If $U_{k,H}(n) = U_k(n) \times H$, then by definition of internal direct product we get $U_k(n) \cap H = \{1\}$. □

Corollary 1.31. *$U_{k,H}(n)/U_k(n) \approx H$ and $U_{k,H}(n)/H \approx U_k(n)$.*

Corollary 1.32. *Let $n = p^m$ for an odd prime p. Let H be a subgroup of $U(n)$. If $H \cap U_{p^i}(p^m) = \{1\}$ for $0 \leq i \leq n$, then $U(n)/U_{p^i,H}(n) \approx Z_{\frac{p^i(p-1)}{|H|}}$.*

Proof. Note that $|U(p^m)/U_{p^i,H}(n)| = \dfrac{p^m(p-1)}{p^{m-i}|H|} = \dfrac{p^i(p-1)}{|H|}$. Since the factor group of a cyclic group is cyclic, the result follows. □

We conclude this section with the following note: in Definition 1.27 we can let H be a subgroup of $U(k)$ instead of $U(n)$. This will yield a subgroup of $U(n)$ but no significant results were discovered due to the "unnatural" nature of this subgroup.

1.6 Results related to $U(n)^{(k)}$

To answer the question of finding the elements of $U(252)$ that form a subgroup isomorphic to $Z_2 \oplus Z_2 \oplus Z_2$, proposed at the end of Section 1.4, we shift our attention to another way of producing subgroups of $U(n)$.

Definition 1.33. *Let $n > 1$ and k be any integer. We define*

$$U(n)^{(k)} = \left\{x^k |\ x \in U(n)\right\}.$$

This defines a subgroup of $U(n)$ (by the finite subgroup test). This is simply raising every element of $U(n)$ to the k-th power and moding the result by n. If k doesn't divide $\phi(n)$, this subgroup can be viewed as the image of the automorphism given by $\phi(x) = x^k$. If k is a divisor of $\phi(n)$, ϕ defines a homomorphism from $U(n)$ to itself the kernel of which is:

$$Ker(\phi) = \left\{x \in U(n) |\ x^k = e\right\}.$$

Example 1.34. Consider $U(13) = \{1, 5, 7, 12\}$ and let $k = 2$. Then $U(13)^{(2)} = \{1, 12, 12, 1\}$. Therefore $U(13)^{(2)} = \{1, 12\}$.

Proposition 1.35. *For $n > 1$ and any integer k, $U(n)^{(k)} = U(n)^{gcd(k,\phi(n))}$.*

Proof. Let $\gcd(k, \phi(n)) = d$ and $k = dh$. Since $U(n)^{(d)}$ and $U(n)^{(k)}$ are both subgroups of $U(n)$, we only need to show they are subsets of each other. Clearly $U(n)^{(k)} \subseteq U(n)^{(d)}$ since $x^{hd} = (x^h)^d$. Now let $x^d \in U(n)^{(d)}$. We know $d = t_1k + t_2\phi(n)$ which implies $x^d = x^{t_1k+t_2\phi(n)} = x^{t_1k} \cdot x^{t_2\phi(n)} = (x^{t_1})^k \in U(n)^{(k)}$. □

Proposition 1.35 allows us to assume the superscript k is always a divisor of $|U(n)| = \phi(n)$.

Example 1.36. Consider $U(252) \approx U(4) \oplus U(9) \oplus U(7) \approx Z_2 \oplus Z_6 \oplus Z_6$. Direct calculations show that $U(252)^{(3)} = \{1, 55, 71, 125, 127, 181, 197, 251\} \approx Z_2 \oplus Z_2 \oplus Z_2$. Observe each element in $U(252)^{(3)}$ has order 2.

Note that in the previous example raising the elements of $U(252)$ to the third power is equivalent to multiplying the elements of $Z_2 \oplus Z_6 \oplus Z_6$ by 3. In order the get the structure of the latter, all we have to do is trace the generator of each group, namely 1, after being multiplied by 3. In the first component, Z_2, 3 mod 2 is 1 therefore we get Z_2. In the next two Z_6 components, $1 \to 3$ which yields a Z_2. To summarize, finding the structure of $U(n)^{(k)}$ is equivalent to following 1 in the cyclic group decomposition of $U(n)$. This is the main idea of Theorem 1.37.

Theorem 1.37. *Let $n = p_1^{m_1} \cdots p_j^{m_j}$ for distinct odd primes p_i and positive integers m_i. Then $U(p_1^{m_1} \cdots p_j^{m_j})^{(k)} \approx Z_{d_1} \oplus \cdots \oplus Z_{d_j}$ where $d_i = \dfrac{\phi(p_i^{m_i})}{gcd(\phi(p_i^{m_i}), k)}$ for all $1 \leq i \leq j$.*

Proof. We know that $U(n) \approx Z_{\phi(p_1^{m_1})} \oplus \cdots \oplus Z_{\phi(p_j^{m_j})}$. Raising every elements in $U(n)$ to the k-th power is equivalent to multiplying all the elements of $Z_{\phi(p_1^{m_1})} \oplus \cdots \oplus Z_{\phi(p_j^{m_j})}$ by k. This is a mapping of cyclic groups back to themselves. One only needs to trace where the generator, 1, of each cyclic component is mapped. Observe that 1 goes to k for each piece. Hence $Z_{\phi(p_i^{m_i})}$ is mapped to Z_{d_i} where $d_i = \dfrac{\phi(p_i^{m_i})}{gcd(\phi(p_i^{m_i}), k)}$. □

Corollary 1.38. *Let $n = 2^b p_1^{m_1} \cdots p_j^{m_j}$ for distinct odd primes p_i and positive integers b and m_i for all i. Define $d_i = \dfrac{\phi(p_i^{m_i})}{gcd(\phi(p_i^{m_i}), k)}$ for all $1 \leq i \leq j$. Then*

1. *$U(2 \cdot p_1^{m_1} \cdots p_j^{m_j})^{(k)} \approx U(p_1^{m_1} \cdots p_j^{m_j})^{(k)} \approx Z_{d_1} \oplus \cdots \oplus Z_{d_j}$.*
2. *$U(2^b p_1^{m_1} \cdots p_j^{m_j})^{(k)} \approx Z_2 \oplus Z_{d_1} \oplus \cdots \oplus Z_{d_j}$ if $b = 2$ and k is odd.*

3. $U(2^b p_1^{m_1} \cdots p_j^{m_j})^{(k)} \approx Z_{d_1} \oplus \cdots \oplus Z_{d_j}$ *if* $b = 2$ *and* k *is even.*

4. $U(2^b p_1^{m_1} \cdots p_j^{m_j})^{(k)} \approx Z_2 \oplus Z_{2^{b-2}} \oplus Z_{d_1} \oplus \cdots \oplus Z_{d_j}$ *if* $b \geq 3$ *and* k *is odd.*

5. $U(2^b p_1^{m_1} \cdots p_j^{m_j})^{(k)} \approx Z_{\frac{2^{b-2}}{gcd(2^{b-2},k)}} \oplus Z_{d_1} \oplus \cdots \oplus Z_{d_j}$ *if* $b \geq 3$ *and* k *is even.*

Proof. For $b = 1$ observe that $U(2 \cdot p_1^{m_1} \cdots p_j^{m_j}) \approx U(p_1^{m_1} \cdots p_j^{m_j})$. If $b = 2$, we have $U(n) \approx Z_2 \oplus Z_{\phi(p_1^{m_1})} \oplus \cdots \oplus Z_{\phi(p_j^{m_j})}$. If k is odd, the additional Z_2 term doesn't change and the rest is identical to Theorem 1.37. If k is even, the first Z_2 is gone because we are mapping 1 to k mod 2 which yields zero. For $b \geq 3$ we get $U(n) \approx Z_2 \oplus Z_{2^{b-2}} \oplus Z_{\phi(p_1^{m_1})} \oplus \cdots \oplus Z_{\phi(p_j^{m_j})}$. For odd k the term $Z_2 \oplus Z_{2^{b-2}}$ stays the same. For even k, the first Z_2 is gone. We need to find the order of $1 \cdot k = k$ in the $Z_{2^{b-2}}$ term to find its structure. But that order is exactly $\frac{2^{b-2}}{gcd(2^{b-2},k)}$ and since every subgroup of a cyclic group is cyclic, the result follows. □

The previous theorem and it's corollary help us find the explicit group elements of various subgroups with desired structures, including p-Sylow subgroups.

Definition 1.39. [3] *Let G be a group and let p be a prime. If p^k divides $|G|$ and p^{k+1} does not divide $|G|$, then any subgroup of G of order p^k is called a Sylow p-subgroup of G.*

Example 1.40. Let $n = 3^3 \cdot 7 \cdot 19$. The cyclic group structure of $U(n)$ is $Z_6 \oplus Z_{18} \oplus Z_{18}$. By Theorem 1.37 we have $U(n)^{(9)} \approx Z_{\frac{6}{gcd(6,9)}} \oplus Z_{\frac{18}{gcd(18,9)}} \oplus Z_{\frac{18}{gcd(18,9)}} \approx Z_2 \oplus Z_2 \oplus Z_2$. Therefore after raising every element of $U(n)$ to the 9th power, we are left with the Sylow 2-subgroup of $U(n)$. Define $\phi : U(n) \to U(n)$ by $\phi(x) = x^9$. We claim $Ker(\phi)$ is the Sylow 3-subgroup of $U(n)$. By the first isomorphism theorem observe that $U(n)/Ker(\phi) \approx (U(n))^{(9)} \approx Z_2 \oplus Z_2 \oplus Z_2$ which implies $Ker(\phi)$ is the collection of all elements of $U(n)$ whose order divides 9 and that is $Z_3 \oplus Z_9 \oplus Z_9$ which is the 3-Sylow subgroup of $U(n)$. Hence $Ker(\phi) \approx Z_3 \oplus Z_9 \oplus Z_9$.

$U(n)^{(2)}$ is a second description of the Sylow 3-subgroup of $U(n)$. By Theorem 1.37 we observe that $U(n)^{(2)} \approx Z_{\frac{6}{gcd(6,2)}} \oplus Z_{\frac{18}{gcd(18,2)}} \oplus Z_{\frac{18}{gcd(18,2)}} \approx Z_3 \oplus Z_9 \oplus Z_9$.

Example 1.41. Suppose in the previous example we wanted to find the exact elements of $U(n)$ that form a subgroup isomorphic to $Z_6 \oplus Z_2$.

Define $H = U_{7\cdot 19}(3^3 \cdot 7 \cdot 19)^{(9)}$ and $K = U_{3^3\cdot 19}(3^3 \cdot 7 \cdot 19)$. Using previous results and Theorem 1.37 it's clear that $U_{7\cdot 19}(3^3 \cdot 7 \cdot 19) \approx Z_{18}$ and therefore $H = U_{7\cdot 19}(3^3 \cdot 7 \cdot 19)^{(9)} \approx Z_2$. Note that $K \approx Z_6$. Let $L = H \times K$. Since $H \cap K = \{1\}$ we get $L \approx H \oplus K \approx Z_2 \oplus Z_6$.

1.7 General Results Related to $U(n)$ Groups

This section includes some known results about $U(n)$ groups and their orders. First we determine the necessary and sufficient conditions on $n > 2$ such that the order of $U(n)$ is the power of a prime. This is a well known number theory result but we include it here for completeness and because the author proved this result independently. The statement of Theorem 1.48 is well-known but our elementary proof of it is original; it employs a blend of group theoretic techniques and number theoretic results. (We are unaware of any other simple proof of this statement besides ours.)

Recall the following from Section 1.2:

$$U(2^n) \approx Z_2 \oplus Z_{2^{n-2}} \text{ for } n \geq 3$$
$$U(p^m) \approx Z_{p^{m-1}(p-1)} \text{ for an odd prime } p.$$

These formulas show for $n > 2$ the order of $U(n)$ is always even and Lemma 1.42 is a direct consequence of them.

Lemma 1.42. *For any $n > 2$, if the order of $U(n)$ is a power of a prime p then $p = 2$.*

Recall the definition of a Fermat prime.

Definition 1.43. *A Fermat number is a positive integer of the form $2^{2^n} + 1$ for some non-negative integer n. A prime of the form $p = 2^{2^n} + 1$ is called a Fermat prime.*

Lemma 1.44. *For an odd prime p the order of $U(p)$ is 2^k for some positive integer k if and only if p is a Fermat prime.*

Proof. Note $|U(p)| = p - 1$ for any odd prime p. If p is a Fermat prime it has the form $p = 2^{2^h} + 1$ and $|U(p)| = 2^{2^h} = 2^k$ where $k = 2^h$. If $|U(p)| = 2^k$ then $p - 1 = 2^k$, which implies $p = 2^k + 1$. Assume for the sake of contradiction that k has an odd divisor m and $k = mn$. Then $p = 2^k + 1 = (2^n)^m + 1 = (2^n + 1)((2^n)^{m-1} - (2^n)^{m-2} + \cdots + 1)$ which is a contradiction because p is a prime and can't be factored. So k can't have any odd factors and therefore $k = 2^h$. □

Theorem 1.45. *For $n > 1$, the order of $U(n)$ is a power of a 2 if and only if $n = 2^m$, $n = q_1 \cdots q_k$ or $n = 2^m \cdot q_1 \cdots q_k$ where $m \geq 2$ and q_i is a Fermat prime for $1 \leq i \leq k$.*

Proof. If n is equal to one of the three cases of the theorem, it follows from formulas in Section 1.2, Lemma 1.42 and Proposition 1.9 that the order of $U(n)$ is a power of 2.

Suppose $|U(n)| = 2^k$ for some $k \geq 1$. Assume for the sake of contradiction that $n \neq 2^m$, $n \neq q_1 \cdots q_k$ or $n \neq 2^m \cdot q_1 \cdots q_k$ where $m \geq 2$ and q_i is a Fermat prime for $1 \leq i \leq k$. Let $n = 2^m \cdot p_1^{n_1} \cdots p_k^{n_k}$ be the prime factorization of n where p_i is an odd prime for all $1 \leq i \leq k$ and at least one p_i is not a Fermat prime. If $n_i \geq 2$ for some i with $1 \leq i \leq k$, we have a contradiction because $|U(n)| = |U(2^m)| \cdot |U(p_1^{n_1})| \cdots |U(p_i^{n_i})| \cdots |U(p_k^{n_k})|$ but $|U(p_i^{n_i})|$ is not a power of 2.

Now suppose $n_i = 1$ for all i so that $n = 2^m \cdot p_1 \cdots p_k$ where p_i is not a Fermat prime for some i with $1 \leq i \leq k$. Then $|U(n)| = |U(2^m)| \cdot |U(p_1)| \cdots |U(p_i)| \cdots |U(p_k)|$. By Proposition 1.9, $|U(p_i)|$ is not a power of 2, which is a contradiction. □

Proposition 1.46. *Let $n > 1$ and H be a subgroup of $U(n)$ that contains all elements of even order. Then $H = U(n)$.*

Proof. We know $U(n) \approx Z_{n_1} \oplus \cdots \oplus Z_{n_k}$ where each n_i is even. Let H be a subgroup of $U(n)$ that contains all elements of even order. Then $H \approx H'$ where H' is a subgroup of

$Z_{n_1} \oplus \cdots \oplus Z_{n_k}$ and contains all elements of even order. Since each n_i is even, H' contains the generator of each Z_{n_i} so we get $H' = Z_{n_1} \oplus \cdots \oplus Z_{n_k}$, which implies $H = U(n)$. □

Proposition 1.47. *There is no positive integer n such that $\phi(n) = 14$.*

Proof. Suppose there is such integer n. Then $U(n) \approx Z_{14}$ since there is only one finite Abelian group of order 14 up to isomorphism. We know that $|U(n)| = \phi(n) = 14$. Let $n = p_1^{n_1} \cdots p_k^{n_k}$ be the prime factorization of n. Then $\phi(n) = p_1^{n_1-1}(p_1 - 1) \cdots p_k^{n_k-1}(p_k - 1)$. Hence 7 divides p_i or $p_i - 1$ for some i. If 7 divides p_i, then $\phi(7)$ divides $\phi(n)$ but 6 does not divide 14. Therefore 7 must divide $p_i - 1$ and we get $p_i = 7k + 1$. We know $7k$ divides 14 but for $k = 1$ we get $p_i = 8$ which is not a prime and for $k = 2$ we get $p_i = 15$ but $\phi(15) \neq 14$ and 15 is not a prime either. □

Proposition 1.47 demonstrates that there are even positive integers k such that there is no U-group of order k. However we can prove that every finite Abelian group is isomorphic to a subgroup of a U-group. We will use the Dirichlet's theorem [6], also called Dirichlet's prime number theorem, which states for any two relatively prime integer a and b, there are infinitely many primes of the form $q = an + b$ where n is a non-negative integer.

Theorem 1.48. *Every finite Abelian group is isomorphic to a subgroup of a U-group.*

Proof. Let G be a finite Abelian group. By the Fundamental Theorem of Finite Abelian Groups G is isomorphic to a group of the form $G \approx Z_{p_1^{a_1}} \oplus \cdots \oplus Z_{p_1^{a_i}} \oplus \cdots \oplus Z_{p_s^{r_1}} \oplus \cdots \oplus Z_{p_s^{r_h}}$ where p_i's are primes and we have arranged the subscripts such that a_1 is the highest exponent of p_1 and r_1 is the highest exponent of p_s. Let $a = p_1^{a_1}$ and $b = 1$ in the statement of Dirichlet's theorem. Then there are infinitely many primes of the form $q = p_1^{a_1} n + 1$ which implies $p_1^{n_1}$ divides $\phi(q)$ and therefore $U(q)$ has a subgroup of order $p_1^{n_1}$. We can find i distinct primes, $q_1, \ldots, q_i$, of the form $p_1^{a_1} n + 1$, each of which will have a subgroup of order $p_1^{n_1}$ and since that was the biggest power of p_1, we can get a subgroup of a smaller power of p_1. Repeat this process for each prime up to p_s and multiply all the primes and we get our desired n. □

2 Extra results/Alternate proofs

Example 2.1. Let $n = 3 \cdot 5 \cdot 7 \cdot 8 = 840$. Then $U_{\pm 105}(840) = \{1, 209, 211, 419, 421, 629, 631, 839\}$. On the other hand $U_{\pm 105}(840) = U_{105}(840) \times \{1, 839\} = \{1, 211, 421, 631\} \times \{1, 839\}$, which yields the set above. Moreover, we see that $U_{105}(840) \approx U(8) \approx Z_2 \oplus Z_2$ and $\{1, 839\} \approx Z_2$. Hence $U_{\pm 105}(840) \approx Z_2 \oplus Z_2 \oplus Z_2$.

Proposition 2.2. *Let $k > 1$ be a divisor of $n = kp^n$ for an odd prime p where gcd$(k, p) = 1$. Then $U_{\pm k}(n) \approx Z_{p^n - p^{n-1}} \oplus Z_2$.*

It follows, from direct calculations, that $U_{\pm k}(2k) \approx Z_2$ and $U_{\pm k}(4k) \approx Z_2 \oplus Z_2$, where k is any odd integer.

Lemma 2.3. *Let $p_1, \ldots, p_k$ $(k > 1)$ be distinct primes. For $m_i \geq 2$, $1 \leq j_i \leq m_i$, and $1 \leq i \leq k$, we have $U_{p_1^{j_1} \cdots p_k^{j_k}}(p_1^{m_1} \cdots p_k^{m_k})$ is a subgroup of $U_{p_1 \cdots p_k}(p_1^{m_1} \cdots p_k^{m_k})$.*

Proof. Let $H = U_{p_1^{j_1} \cdots p_k^{j_k}}(p_1^{m_1} \cdots p_k^{m_k})$ and $K = U_{p_1 \cdots p_k}(p_1^{m_1} \cdots p_k^{m_k})$. Let $x \in H$, then $x \equiv 1 \pmod{p_1^{j_1} \cdots p_k^{j_k}}$ where $j_i \geq 1$ for all i. Therefore $x \equiv 1 \pmod{p_1 \cdots p_k}$. □

Lemma 2.4. *Let $p_1, \ldots, p_k$ $(k > 1)$ be distinct primes. For $m_i \geq 2$, $1 \leq j_i \leq m_i$, and $1 \leq i \leq k$, we have $|U_{p_1^{j_1} \cdots p_k^{j_k}}(p_1^{m_1} \cdots p_k^{m_k})| = p_1^{m_1 - j_1} \cdots p_k^{m_k - j_k}$.*

Proof. For convenience let $s = p_1^{m_1} \cdots p_k^{m_k}$, $t = p_1^{j_1} \cdots p_k^{j_k}$ and $H = U_{p_1^{j_1} \cdots p_k^{j_k}}(p_1^{m_1} \cdots p_k^{m_k})$. By definition $H = \left\{1, t+1, 2t+1, \cdots (p_1^{m_1 - j_1} \cdots p_k^{m_k - j_k} - 1)t + 1\right\}$. Note each element in H is relatively prime to s. For every prime p_i in s, any element x in H is 1 plus a multiple of p_i and hence x relatively prime to s. By definition elements in H are less than s, relatively prime to t and s, and there are exactly $p_1^{m_1 - j_1} \cdots p_k^{m_k - j_k}$ such multiples. □

Before stating the next theorem, we need the following definition.

Definition 2.5. ***(Legendre formula)*** *For any positive integer n and prime p, let $\mathcal{V}_p(n!)$ be the largest power of p that divides $n!$,*

$$\mathcal{V}_p(n!) = \sum_{i=1}^{i=\infty} \left\lfloor \frac{n}{p^i} \right\rfloor$$

where $\lfloor x \rfloor$ is the floor function.

From the definition above and using the formula for a geometric sum, we see that for an odd prime p and $n \geq 4$:

$$\mathcal{V}_p(n!) < \sum_{i=1}^{i=\infty} \frac{n}{p^i} = \frac{n}{p-1} \leq n-2.$$

Note if $n = 3$ and p is an odd prime, $\mathcal{V}_p(n!) \leq n-2$. We include this and two more well-known number theory results in the following lemma.

Lemma 2.6. *For $n \geq 3$ and p an odd prime, $\mathcal{V}_p(n!) \leq n-2$. If n is not a power of 2, then $\mathcal{V}_2(n!) \leq n-2$. If $n = 2^k$ then $\mathcal{V}_2(n!) = 2^k - 1$. (needs citation.)*

Theorem 2.7. *Let $p_1, \ldots, p_k$ be distinct odd primes. For $2 \leq m_i$ and $1 \leq j_i \leq m_i$, for all $1 \leq i \leq k$, we have $U_{p_1^{j_1} \cdots p_k^{j_k}}(p_1^{m_1} \cdots p_k^{m_k}) \approx Z_{p_1^{m_1-j_1} \cdots p_k^{m_k-j_k}}$.*

Proof. If $m_i = j_i$ for all indices i, the result is trivial. Suppose $j_i < m_i$ for at least one i. By Lemma 2.3 it suffices to show $U_{p_1 \cdots p_k}(p_1^{m_1} \cdots p_k^{m_k}) \approx Z_{p_1^{m_1-1} \cdots p_k^{m_k-1}}$. That is to show $H = U_{p_1 \cdots p_k}(p_1^{m_1} \cdots p_k^{m_k})$ is cyclic. For convenience let $a = p_1^{m_1} \cdots p_k^{m_k}$ and $x = p_1 \cdots p_k$. Recall H is a subgroup of $U(a)$ so the operation is multiplication mod a. From Lemma 2.4 we have $|H| = p_1^{m_1-1} \cdots p_k^{m_k-1}$, so H has the desired cardinality. We will show $x+1$ is the generator of H. It follows from Lagrange's theorem that $(x+1)^{|H|} = 1$. Let $b = p_1^{m_1-1} \cdots p_i^{m_i-2} \cdots p_k^{m_k-1}$ for some $1 \leq i \leq k$. We will show $(x+1)^b \neq 1 \pmod{a}$. This will prove $|x+1| = |H|$.

Consider

$$(x+1)^b = \binom{b}{0}x^b + \cdots + \binom{b}{b-1}x + 1.$$

Observe that $\binom{b}{b-1}x+1 = p_1^{m_1}\cdots p_i^{m_i-1}\cdots p_k^{m_k}+1 \neq 1 \pmod a$ hence sum of the last two terms is non-zero and not 1 mod a. We will show $\binom{b}{b-d}x^d = 0 \pmod a$ for all $2 \leq d \leq b$.

For $d=2$, $\binom{b}{b-2}x^2 = \dfrac{b(b-1)}{2}x^2$. Since b is odd 2 divides $(b-1)$ and a is a factor of bx^2, hence this term is zero mod a.

For $d \geq 3$, $\binom{b}{b-d}x^d = \dfrac{(b)\cdots(b-d+1)}{d!}x^d$. If $d!$ doesn't contain a factor of b, then we are done because $b \cdot x^d$ contains a as a factor. If $d!$ contains prime factors of b, the same factors divide x^d. Note by Lemma 2.6, $\mathcal{V}_p(d!) \leq d-2$ for any odd prime p and $d \geq 3$. Hence we will always have *at least* x^2 left in which case bx^2 contains a as a factor and this term is $0 \pmod a$. Therefore $\binom{b}{b-d}x^d \equiv 0 \pmod a$ for all $d \geq 3$. Note there is always an excess of prime factors left in x than needed to make a a factor and this is a worst case scenario analysis. So we have shown $(x+1)^b \neq 1 \pmod a$ where $b = p_1^{m_1-1}\cdots p_i^{m_i-2}\cdots p_k^{m_k-1}$ and $1 \leq i \leq k$. Therefore $|x+1| = |H|$. □

Corollary 2.8. *Let $p_1, \ldots, p_k$ be k distinct primes. For $3 \leq m_i$, $2 \leq j_i \leq m_i$, where $1 \leq i \leq k$, we have $U_{p_1^{j_1}\cdots p_k^{j_k}}(p_1^{m_1}\cdots p_k^{m_k}) \approx Z_{p_1^{m_1-j_1}\cdots p_k^{m_k-j_k}}$.*

Proof. The difference in the corollary is that it includes 2 as a prime and the lower bound on m_i's and j_i's are different. By Lemma 2.3 we need to show $U_{2^2\cdots p_k^2}(2^{m_1}\cdots p_k^{m_k})$ is isomorphic to $Z_{2^{m_1-2}\cdots p_k^{m_k-2}}$. For convenience let $H = U_{2^2\cdots p_k^2}(2^{m_1}\cdots p_k^{m_k})$, $a = 2^{m_1}\cdots p_k^{m_k}$ and $x = 2^2\cdots p_k^2$. By Lemma 2.4, $|H| = 2^{m_1-2}\cdots p_k^{m_k-2}$ and by Lagrange's theorem $(x+1)^{|H|} = 1 \pmod a$. Now let $b = p_1^{m_1-2}\cdots p_i^{m_i-3}\cdots p_k^{m_k-2}$. Since we've done the odd case above, let $p_i = 2$. Then $b = 2^{m_1-3}\cdots p_k^{m_k-2}$. The sum of last two terms of the binomial expansion of $(x+1)^b$ are $2^{m_1-1}\cdots p_k^{m_k}+1$ which are non-zero and not 1 when we mod by a. We will show $\binom{b}{b-k}x^k$ is $0 \pmod a$ for all $2 \leq k \leq b$. For $k=2$, we have $\dfrac{(b)(b-1)}{2}x^2$. Then b contains a factor of 2^{m_1-4} but x^2 has a factor of 2^4 hence this term is

$0 \pmod{a}$.

For $k \geq 3$, we have

$$\frac{(b)\cdots(b-k+1)}{k!}x^k.$$

If k is not a power of 2, then $\mathcal{V}_2(k!) \leq k-2$, hence $\dfrac{x^k}{k!}$ has 2^{2k-k+2} factors of 2 and we get a 2^{m_1-3} from b which all adds up to 2^{m_1+k-1} and since $k \geq 3$ we have a factor of a and this term is $0 \pmod{a}$.

If $k = 2^n$, by Lemma 2.6, $\mathcal{V}_2(k!) = 2^n - 1$ then $\dfrac{x^k}{k!}$ yields $2^{2(2^n)-2^n-1} = 2^{2^n-1}$. Accounting for b we have $2^{m_1+2^n-4}$. Since $k \geq 3$ then $n \geq 2$ and we get a factor of a which implies this term is $0 \pmod{a}$. □

Corollary 2.9. *Let $p_1, \ldots, p_k$ be k distinct odd primes. For $2 \leq m_i$ and $1 \leq j_i \leq m_i$, for all $1 \leq i \leq k$, it follows that $U_{\pm p_1^{j_1}\cdots p_k^{j_k}}(p_1^{m_1}\cdots p_k^{m_k}) \approx Z_{p_1^{m_1-j_1}\cdots p_k^{m_k-j_k}} \oplus Z_2$.*

Corollary 2.10. *let $p_1, \ldots, p_k$ be k distinct primes. For $3 \leq m_i$ and $2 \leq j_i \leq m_i$ for all $i = 1, \ldots, k$, we have $U_{\pm p_1^{j_1}\cdots p_k^{j_k}}(p_1^{m_1}\cdots p_k^{m_k}) \approx Z_{p_1^{m_1-j_1}\cdots p_k^{m_k-j_k}} \oplus Z_2$.*

Theorem 2.7 and its corollaries do not address the case of $U_{2k}(2^m k)$ where k is an odd integer. It follows, from definition, that $U_{2k}(2k) \approx Z_1$ and $U_2 k(4k) \approx Z_2$.

Proposition 2.11. *Let k be an odd integer and $m \geq 3$. Then $U_{2k}(2^m k) \approx Z_{2^{m-2}} \oplus Z_2$*

Proof. It is clear that $U_{2k}(2^m k) = U_k(2^m k)$ (because $gcd(mk+1, 2^m k) \neq 1$ when m is odd). From previous formulas we have $U_k(2^m k) \approx U(2^m) \approx Z_{2^{m-2}} \oplus Z_2$. □

3 Conclusion and Further Research

For positive integers n and k we have fully classified, in terms of external direct products of cyclic groups, all subgroups of $U(n)$ of the form $U_k(n)$, $U_{\pm k}(n)$ and the factor group $U(n)/U_k(n)$. We can use our classification methods, mainly Theorem 1.13, to pull back to $U(n)$ and find specific group elements that form a subgroup with a desired cyclic group decomposition. However the structure of $U(n)/U_{\pm k}(n)$ is an open question.

We have provided partial classification results on the more general class of subgroups of the form $U_{k,H}(n)$ where k is a divisor of n and H is a subgroup of $U(n)$. We were unable to find the structure of $U_{k,H}(n)$ when the intersection of $U_k(n)$ and H is nontrivial. It is an open question whether every subgroup of $U(n)$ has a non-trivial construction of the form $U_{k,H}(n)$? If not, then which subgroups of $U(n)$ have such construction? Note that for a subgroup H of $U(n)$, a trivial construction would be $U_{n,H}(n)$. It remains an open question to determine the structure of $U(n)/U_{k,H}(n)$.

Our results fully classify subgroups of the form $U(n)^{(k)}$. The results related to $U(n)^{(k)}$ provide an algorithm for finding group elements of $U(n)$ that form the Sylow p-subgroups; combined with the aforementioned results allow us to find group elements of $U(n)$ that form a specific direct products of cyclic groups.

All of the results in Section 1.7 are well known. Although the order of $U(n)$ for any integer $n > 2$ is even, not all even numbers are the order of a $U(n)$ group. The smallest example is 14, which we showed in Proposition 1.47. Which even numbers are the order of a $U(n)$ group is unknown. Another long standing problem is finding a generator of a $U(n)$ group. These generators are called “primitive roots" in number theory. To the best of my knowledge, there is no fast way or algorithm to find a generator by hand. There are several computer algorithms that are relatively quick.

Finally, it would be interesting to look for the structure of the group of units of the ring $\mathbb{Z}[\rho]$ where ρ is the primitive n-th root of unity.

4 References

[1] Adam A. Allan, Micheal J. Dunne, John R. Jack, Justin C. Lynd and Harold W. Ellingsen Jr, Classification of the group of units in Gaussian integers modulo n, *Pi Mu Epsilon Journal* 12 (9) (Fall 2008), 513-519.

[2] Y. Cheng, Decompostions of U-groups, *Mathematics Magazine* 62 (1989), 271-273.

[3] Joseph A. Gallian, "Contemporary Abstract Algebra," Ninth Edition, Cengage Learning Boston, 2017.

[4] Joseph A. Gallian and D. Rusin, Factoring groups of integers modulo n, *Mathematics Magazine* 53 (1980), 33-36.

[5] Emily Gullerud and Aba Mbirika, An Euler phi function for Eisenstein integers and some applications, arXiv:1902.03483.

[6] D. Shanks, "Solved and Unsolved Problems in Number Theory," 2nd ed., New York: Chelsea, 1978.